



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,919	12/22/2003	David Carroll Challenger	RPS920030244US1	8405
63203 7590 10/10/2007 ROGITZ & ASSOCIATES 750 B STREET SUITE 3120 SAN DIEGO, CA 92101			EXAMINER YOUNG, NICOLE M	
			ART UNIT 2139	PAPER NUMBER
			MAIL DATE 10/10/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/748,919
Filing Date: December 22, 2003
Appellant(s): CHALLENGER ET AL.

MAILED

GCT 1 U 2007

Technology Center 2100

John L. Rogitz
Registration No. 33,549
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10 July 2007 appealing from the Office action mailed 22 June 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The 112 rejections of claims 1-22 for antecedent basis have been withdrawn.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2003/0142641

Sumner et al.

7-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-22 are rejected under 35 U.S.C. 102(e) as being anticipated by **Sumner et al (US 2003/0142641)** hereinafter referred to as Sumner.

Claims 1 and 14 disclose a service and a system comprising:

determining that a mobile computer has lost connectivity to a first access point of a

network; (paragraph [0060], "when a predefined drop in throughput is reached)

when the mobile computer roams (paragraph [0060] "roaming among Access Points of

a WLAN is built into the WLAN card) to a second access point of the network,

determining whether the second access point is authorized for secure communication

and if so (scans frequencies for WLANs with a particular SSID.....user-unique logon

data with a password),

Art Unit: 2139

releasing access to secure data on the network through the second access point (paragraph [0061], "reads about hotel change on his palmtop computer" and paragraph [0062]).

Also relevant is paragraph [0066] where hotel connection is lost, the company WLAN is detected, logged on to, and company files are accessed.

Claims 2 and 15 disclose the service and system of Claims 1 and 14, wherein the service or means is undertaken by the mobile computer (paragraph [0073] "may be implemented in hardware or software, or a combination of both.....implemented in computer programs executing on one or more programmable computersor for the wireless device a low-power microcomputer").

Claims 3 and 16 disclose the service and system of Claims 2 and 15, wherein the service or means is undertaken by a hypervisor in the mobile computer (paragraph [0075] discloses a "special purpose programmable computer" and computers configured to operate in "a specific and predefined manner." The Specification defines a "hypervisor" to be a security module "that is a dedicated part of the CPU chip" [page 4 paragraph 2]. The Examiner interprets computer programs to implement the authentication service or system defined above to be a hypervisor).

Claims 4 and 17 disclose the service and system of Claims 1 and 14, wherein the service or means is undertaken by at least one network resource outside the mobile computer (paragraph [0073] "may be implemented in hardware or software, or a combination of both.....implemented in computer programs executing on one or more

Art Unit: 2139

programmable computers for the infrastructure elements (control point, gateway, databases and access points).

Claims 5 and 18 disclose the service and system of Claims 1 and 14, wherein the mobile computer is authenticated at the first access point, prior to losing connectivity thereto (paragraphs [0056] and [0057] disclose authentication to the airport's WLAN before losing connectivity).

Claim 6 discloses service of Claim 5 wherein releasing access to secure data on the network through the second access point comprises releasing access to a set of secure data which differs from the secure data released when the mobile computer is connected to the first access point (paragraph [0066] where hotel connection is lost, the company WLAN is detected, logged on to, and company files are accessed through the company database and file server which were not previously accessible through the hotel connection).

Claim 7 discloses a mobile computer, comprising:

at least one processor (paragraph [0073] "that each include a processor");

at least one wireless transceiver in communication with the processor, the processor executing logic including ("a wireless transceiver....and software to enable switching between WLANs based on control messages received from a control point associated with a WWAN");

determining whether a predetermined communication hardware event has occurred (paragraph [0063] determining connection lost, "WLAN coverage is lost"); and

if a predetermined communication hardware event has occurred, selectively configuring the computer in a non-secure mode (paragraph [0063] "enters a doze or sleep mode").

Claim 8 discloses the computer of Claim 7, wherein the computer cannot access secure data on the network while configured in said non-secure mode (paragraph [0063] while the mobile device is in sleep or doze mode it cannot authenticate to a network).

Claim 9 discloses the computer of Claim 7, wherein the computer can access a subset of the secure data on the network while configured in said non-secure mode (paragraph [0065], "he could have waited until another e-mail notice came over the paging channel" this would happen while the computer was in sleep/doze mode and in interpreted as a subset of secure data on the network while in non-secure mode).

Claim 10 discloses the computer of Claim 7, wherein the predetermined hardware event is a disconnection from a wireless access point (paragraph [0063] determining connection lost, "WLAN coverage is lost").

Claim 11 discloses the computer of Claim 7, wherein the computer is configured in the nonsecure mode if the computer roams to an access point that is not authorized for secure data transmission (paragraph [0060], while disconnected (interpreted to be nonsecure mode as it is not authenticated) the mobile device roams for WLANs with a certain SSID to authenticate with; if the access point does not have the SSID it is looking for it is not authorized).

Claim 12 discloses the computer of Claim 10, wherein the processor accesses a list of authorized access points to undertake the act of selectively configuring (paragraph [0070] "If the client Tom is visiting has negotiated with his WAN Provide the SSID and

WEP Key, if any for the client's WLAN are available through a central provisioning point.

Tom's WAN provider supplies a list of WLANs to Tom's pager/WLAN card).

Claim 13 discloses the computer of Claim 10, wherein the processor receives a network signal from a wireless access point to indicate whether the wireless access point is an authorized access point to undertake the act of selectively configuring (paragraph [0065], when he card scans for service it will receive a signal from the hotel WLAN indicating it is authorized for connection).

Claim 19 discloses a method comprising:

establishing communication between a mobile computer and a network through an access point (paragraphs [0056] and [0057] disclose authentication to the airport's WLAN);

and based on at least one of: a location, and an identification, of the access point, selectively granting the computer access to secure assets in the network (paragraph [0060] discloses roaming to "several different WLAN Access Points" while in motion because the range of each Access Point is "100-300 feet"; the Access Points also have to meet the criteria of having a particular SSID, an identification).

Claim 20 discloses the method of Claim 19, wherein the act of selectively granting is undertaken by the mobile computer (paragraph [0073] "may be implemented in hardware or software, or a combination of both.....implemented in computer programs executing on one or more programmable computersor for the wireless device a low-power microcomputer").

Claim 21 discloses the method of Claim 20, wherein the act of selectively granting is undertaken by a hypervisor in the mobile computer (paragraph [0075] discloses a "special purpose programmable computer" and computers configured to operate in "a specific and predefined manner." The Specification defines a "hypervisor" to be a security module "that is a dedicated part of the CPU chip" [page 4 paragraph 2]. The Examiner interprets computer programs to implement the authentication service or system defined above to be a hypervisor).

Claim 22 discloses the method of Claim 19, wherein the computer is configured to access a first set of network assets when communicating through a first access point and a second set of network assets when communicating through a second access point (paragraph [0066] where hotel connection is lost, the company WLAN is detected, logged on to, and company files are accessed through the company database and file server which were not previously accessible through the hotel connection).

(10) Response to Argument

In response to the Appellant's argument that Sumner does not teach the level of access based on access point, the Examiner disagrees. As noted in the previous office action, and again above, Sumner paragraph [0060] discloses "scanning frequencies for WLANs with a particular SSID (or an SSID of "ANY"), and then the card tries to connect and log on". Logging on "can be proprietary and occurs at an application level to a logon server, and the user sends the user-unique logon data with a password. Where WEP is used, all cards that can connect to a particular WLAN have the same WEP key by definition." When the card finds an access point it can log on to, for example access

point with an SSID of "ANY", it logs onto a lower level of security than when it finds an access point to log on to where the card uses the WEP enabled user-unique logon data and password. A WLAN with WEP enabled security is higher security level data.

In response to the Appellant's argument regarding claim 7 that the reference does not teach determining whether a predetermined communication hardware event has occurred and if so selectively configuring the computer in a non-secure mode in which data on a network is accessed by the computer but not all secure data available on the network can be accessed by the computer, the Examiner disagrees. Sumner paragraph [0063] teaches determining the connection is lost, "WLAN coverage is lost". The connection being lost is the predetermined communication hardware event and the computer enters a doze mode which cannot access secure data. On the drive to the hotel a notice is sent that new email has been received. This email notice is the data accessed by the computer in from the network when it is in nonsecure mode.

In response to the Appellant's argument regarding claim 19 that the reference does not teach using a location or identification of an access point to decide whether to grant access to secure assets in the network or to grant the computer access to other than the secure assets in the network, the Examiner disagrees. Sumner paragraph [0060] teaches "the card scans frequencies for WLANs with a particular SSID (or an SSID of "ANY"), and then the card tries to connect and log on. The SSID is the identification of the WLAN. If the computer logs on to a WLAN with WEP security enabled it logs on to it with a user-unique password. The data accessed on a WLAN with an SSID of "ANY" and no WEP security enabled with be different and less secure

than the data accessed on a WLAN with a specific SSID and WEP security enabled.

These WLANs are second access points that are authorized for communication and the WEP security enabled WLAN is authorized for secure communication.

In response to the Appellant's argument regarding that the reference does not teach releasing access to secure data on the network through the second access point, the Examiner disagrees. Sumner paragraph [0061] teaches "reads about hotel change on his palmtop computer". This information would be secure data accessed through the second access point. Additionally, in paragraph [0065] Sumner teaches connecting to a WLAN through the hotel's WEP security. The hotel WLAN is another second secure access point. Here the computer is able to connect to a company database and file server. This is accessing information from the first secure access point from a secure second access point. After leaving the hotel the connection is again lost. Paragraph [0066] teaches that when in range the computer logs onto the field office WLAN with a separate SSID and WEP key. Here the computer is able to access IM's from coworkers and requisition files, local files, and corporate files from the company's database and file server. This would be another instance of a second access point releasing secure data, the company IM's and files. The above comments apply to all limitations of claims 1 and 14 as well.

In response to the Appellant's argument regarding claims 3, 16, and 21 that the reference does not teach a hypervisor, the Examiner disagrees. Sumner paragraph [0075] teaches a "special purpose programmable computer" and computers configured to operate in "a specific and predefined manner." The Examiner's broadest possible

Art Unit: 2139

interpretation is that this is a special operating system that operates on top of the standard operating system.

In response to the Appellant's argument regarding claims 6, 9, and 22 that the reference does not teach secure data that is released when the mobile computer is connected to another access point, the Examiner disagrees. Sumner paragraph [0061] teaches "reads about hotel change on his palmtop computer". This information would be secure data accessed through the second access point. Additionally, in paragraph [0065] Sumner teaches connecting to a WLAN through the hotel's WEP security. The hotel WLAN is another second secure access point. Here the computer is able to connect to a company database and file server. This is accessing information from the first secure access point from a secure second access point. After leaving the hotel the connection is again lost. Paragraph [0066] teaches that when in range the computer logs onto the field office WLAN with a separate SSID and WEP key. Here the computer is able to access IM's from coworkers and requisition files, local files, and corporate files from the company's database and file server. This would be another instance of a second access point releasing secure data, the company IM's and files. The above comments apply to all limitations of claims 1 and 14 as well.

The 112 rejections of claims 1-22 have been withdrawn.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Art Unit: 2139

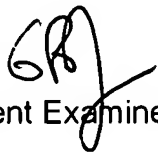
Respectfully submitted,

Nicole Young
Patent Examiner
Art Unit 2139

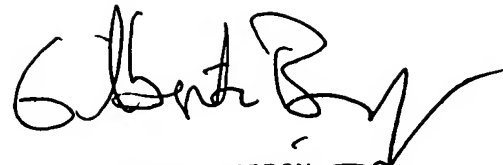


Conferees:

Gilberto Barron
Supervisory Patent Examiner
Art Unit 2132



/Benjamin Lanier/
Benjamin Lanier
Patent Examiner
Art Unit 2132



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100